EXHIBIT A

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Boulevard, Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
E-Mail: ltfisher@bursor.com

BURSOR & FISHER, P.A.
Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-mail: pfraietta@bursor.com

Attorneys for Plaintiffs

SUPERIOR COURT OF THE STATE OF CALIFORNIA

FOR THE COUNTY OF SANTA CLARA

ALAN STARZINSKI, OLADEJI ODUMOSU, AURELIO MEDINA, and DARRNELL MCCOY, individually and on behalf of all others similarly situated,

Plaintiffs,

v.

META PLATFORMS, INC., fka FACEBOOK, INC.,

Defendant.

Case No. 24CV441982

CLASS ACTION

COMPLAINT

Plaintiffs Alan Starzinski, Oladeji Odumosu, Aurelio Medina, and Darrnell McCoy ("Plaintiffs"), on behalf of themselves and all other persons similarly situated, by and through their attorneys, make the following allegations pursuant to the investigation of their counsel and based upon information and belief, except as to allegations specifically pertaining to themselves, which are based on personal knowledge.

NATURE OF THE ACTION

1. This is a class action brought on behalf of all persons with Facebook accounts who subscribe to Paramount+, ESPN+, Hulu, and Starz (together, the "Streaming Services").

2. Plaintiff Starzinski also brings this suit on behalf of all persons with a Paramount+ subscription (the "Paramount Subclass").

3. Plaintiffs Odumosu and Monserrat also bring this suit on behalf of all persons with an ESPN+ subscription (the "ESPN Subclass").

4. Plaintiffs Odumosu and Medina also bring this suit on behalf of all persons with a Hulu subscription (the "Hulu Subclass").

5. Plaintiff McCoy also brings this suit on behalf of all persons with a Starz subscription (the "Starz Subclass").

6. Meta Platforms, Inc. ("Defendant" or "Facebook") develops, owns, and operates the largest social networking platform on the planet.

7. Facebook intentionally intercepted Plaintiffs' and Class members' electronic communications. Facebook failed to receive consent for these interceptions, instead obfuscating the volume, specificity, and type of data it intercepted and collected.

8. Facebook also intentionally intercepted sensitive and confidential communications between the Streaming Services and its subscribers. Facebook likewise failed to receive consent for these interceptions, having engaged in conduct that expressly contravened its own terms and representations.

9. By failing to first receive consent before intercepting and collecting electronic communications, Facebook violated California law as described herein.

BACKGROUND

I. FACEBOOK: FROM SOCIAL UTILITY TO TRACKING APPARATUS

10. Facebook is the largest social media site on the planet, touting 2.9 billion monthly active users.[1]

11. Launched in February 2004, the social media site flourished immediately. Within 10 months of its debut, the site reached 1 million active users,[2] quickly swelling to 30 million less than three years later.[3] As its user base grew, so did interest from investors. By late 2007, interest turned to clamor, and after rejecting a steady flow of proposed investments[4] and buyouts,[5] the still nascent company settled on an offer from Microsoft, agreeing to a $240 million investment for a 1.6 percent stake, which extrapolated to an eye-popping valuation: $15 billion.[6]

12. Commentators scrutinized the deal, pointing to the gaping disparity between Facebook's valuation and Facebook's revenue. "When a startup shows an estimated $150 million in revenue, isn't wildly profitable, and doesn't have a clear revenue model, no company in its right mind would give it a $15 billion valuation – except, it seems, if we're talking about Facebook."[7] In short order, Facebook set about crafting that revenue model.

13. Because Facebook offered access to its platform for free, users were exactly that—users, not customers. Rather than find a way to make them customers, Facebook made them the

---

[1] Sean Burch, *Facebook Climbs to 2.9 Billion Users, Report 29.1 Billion in Q2 Sales*, YAHOO (July 28, 2021), https://www.yahoo.com/now/facebook-climbs-2-9-billion-202044267.html.

[2] The Associated Press, *Number of active users at Facebook over the years*, YAHOO FINANCE (Oct. 23, 2012), https://finance.yahoo.com/news/number-active-users-facebook-over-years-214600186--finance.html;

[3] Laura Locke, *The Future of Facebook*, TIME (July 17, 2021), http://content.time.com/time/business/article/0,8599,1644040,00.html.

[4] Nicholas Carlson, *11 companies that tried to buy Facebook back when it was a startup*, BUS. INSIDER (May 15, 2010), https://www.businessinsider.com/all-the-companies-that-ever-tried-to-buy-facebook-2010-5.

[5] Kate Duffy, *When Yahoo offered $1 billion to buy Facebook, Mark Zuckerberg said he wouldn't know what to do with the money and would probably just build another Facebook, a new book says*, BUS. INSIDER (Jul. 14, 2021), https://www.businessinsider.com/an-ugly-truth-mark-zuckerberg-facebook-yahoo-offer-money-book-2021-7.

[6] Brad Stone, *Microsoft Buys Stake in Facebook*, N.Y. TIMES (Oct. 25, 2007), https://www.nytimes.com/2007/10/25/technology/25facebook.html.

[7] Julie Sloane, *Facebook Got Its $15 Billion Valuation – Now What?*, WIRED (Oct. 26, 2007), https://www.wired.com/2007/10/facebook-future/.

products. Facebook planned to mine its platform and third-party websites for insights it could use to target and customize advertisements for businesses.[8] User activity served as the raw materials, materials that Facebook analyzed and dissected for inferences answering its ultimate question: what advertisement, from which company, for which user, will have maximal impact. The better Facebook could answer that question, the better it could "improve the effectiveness of the ads and recruit new advertisers who want to pitch their messages to refined slices of the online audiences."[9] Facebook announced this new business model on November 6, 2007.

14. As that date approached, details leaked about its soon-to-be launched advertising system, with one clear takeaway: "Facebook is going to be gunning hard to get lots and lots of third party data about its users into its database."[10] Facebook quickly dispelled any doubts about that takeaway's veracity. On November 6th, Facebook unveiled its new ad system, "Facebook Ads," pitching it as a way "for businesses to connect with users and target advertising to the exact audiences they want."[11] The new system had three component parts: Social Ads, which let businesses build Facebook pages and create advertisements featuring a user's interaction with those pages; Insights, which let businesses track how those social ads spread among users; and the Beacon program.[12]

II. THE BEACON PROGRAM

15. Facebook extolled the Beacon program as "an advertising breakthrough."[13] The program constituted Facebook's first foray into tracking user activity off its site, piloting the program with 44 business partners who agreed to integrate Facebook's code into their website. The

---

[8] Brad Stone, *MySpace to Discuss Effort to Customize Ads*, N.Y. TIMES (Sept. 18, 2007), https://www.nytimes.com/2007/09/18/technology/18myspace.html.

[9] Brad Stone, *MySpace mines data to tailor advertising*, N.Y. TIMES (Sept. 18, 2007), https://www.nytimes.com/2007/09/18/technology/18iht-social.1.7545453.html.

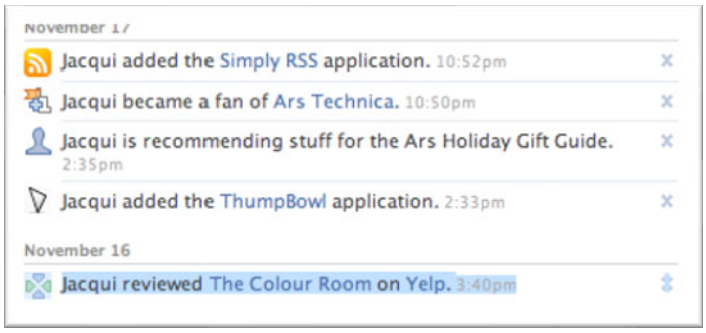
[10] Michael Arrington, *Ok Here's at Least Part of What Facebook Is Announcing On Tuesday: Project Beacon*, TECHCRUNCH (Nov. 2, 2007), https://techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday/.

[11] FACEBOOK, FACEBOOK UNVEILS FACEBOOK ADS, https://about.fb.com/news/2007/11/facebook-unveils-facebook-ads/.

[12] Aline van Duyn and Kevin Allison, *'Facebook ads' to change way of marketing*, FIN. TIMES (Nov. 6, 2007), https://www.ft.com/content/01341240-8cbd-11dc-b887-0000779fd2ac.

[13] The Associated Press, *About-Face For Facebook*, CBS NEWS (Dec. 5, 2007), https://www.cbsnews.com/news/about-face-for-facebook/.

code ran on specific pages, like order confirmation, recording activity and transmitting it to Facebook, which then "report[ed] those activities back to the users' Facebook friends, unless specifically told not to do so."[14] So, for example, if a Facebook user navigated to fandango.com, a partner website, and purchased a movie ticket, Facebook tracked that activity and sent "a notice about what movie they are seeing in the News Feed on all of their friends' pages."[15] The same process applied to all partners, like Yelp:



16. Partners and Facebook both benefitted from this arrangement. For Facebook's part, it received "incredibly valuable data from the user" that it could repurpose "to serve targeted (highly, highly targeted) ads back to them in various other places on Facebook and elsewhere."[16] Businesses supplied this data without compensation, but in return they received a "trusted referral" for their product, considered "the Holy Grail of advertising."[17] "Nothing influences people more than a recommendation from a trusted friend," Facebook's CEO, Mark Zuckerberg, noted.[18] Partners considered this a major selling point, as Blockbuster flaunted in a presentation to investors:

---

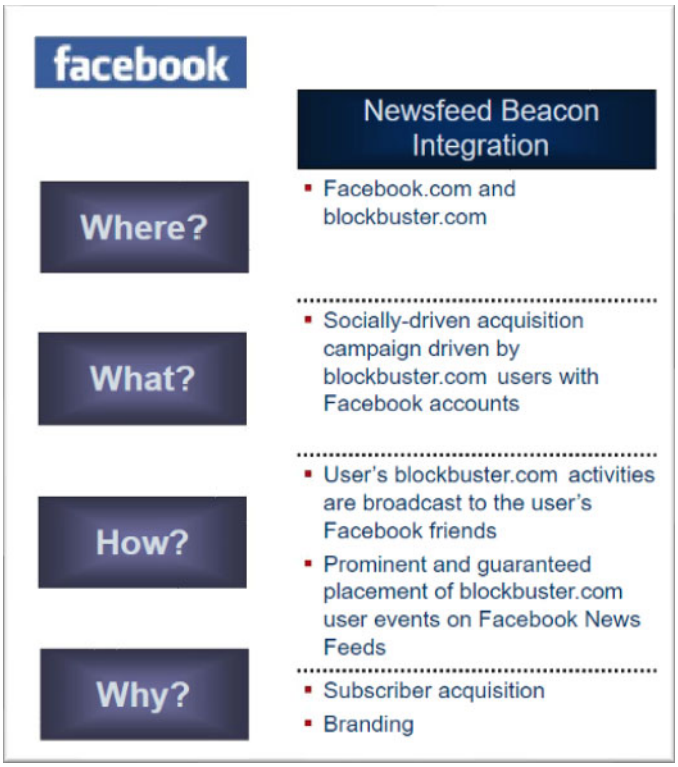
[14] Jaikumar Vijayan and Heather Havenstein, *Facebook's Beacon just the tip of the privacy iceberg,* COMPUTERWORLD (Dec. 3, 2007), https://www.computerworld.com/article/2538002/facebook-s-beacon-just-the-tip-of-the-privacy-iceberg.html.

[15] Louise Story and Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), https://www.nytimes.com/2007/11/30/technology/30face.html.

[16] Michael Arrington, *Ok Here's At Least Part Of What Facebook Is Announcing on Tuesday: Project Beacon*, TECHCRUNCH (Nov. 2, 2007), https://techcrunch.com/2007/11/02/ok-heres-at-least-part-of-what-facebook-is-announcing-on-tuesday/.

[17] Aline van Duyn and Kevin Allison, *'Facebook ads' to change way of marketing*, FIN. TECH (Nov. 6, 2007), https://www.ft.com/content/01341240-8cbd-11dc-b887-0000779fd2ac.

[18] *Id.*



17. The Beacon program was "an important test of online tracking,"[19] but not for its novelty. Companies already tracked users pervasively across the internet, but they did it "behind the scenes, where consumers do not notice it."[20] With the Beacon program, Facebook showcased its tracking program, providing a window into what and how much data it collected on other websites. This fact, Facebook thought, would prove insignificant. "With time, Facebook says, users will accept Beacon, which Facebook views as an extension of the type of book and movie recommendations that members routinely volunteer on their profile pages."[21]

18. Public outrage was swift and overwhelming. Less than a month after the Beacon's introduction, 50,000 users signed an online petition in protest.[22] "Facebook, they say, should not be

[19] Louise Story and Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), https://www.nytimes.com/2007/11/30/technology/30face.html.
[20] *Id.*
[21] *Id.*
[22] *Id.*

following them around the Web, especially without their permission."[23] As the outrage continued to crescendo, Facebook sought to allay concerns by "reassur[ing] users that it only tracks and publishes data about their purchases if they are both logged in to Facebook and have opted-in to having this information listed on their profile."[24]

19. That turned out to be false. "[I]n 'extremely disconcerting' findings that directly contradict these assurances, researchers at CA's Security Advisory service … found that data about these transactions are sent to Facebook regardless of a user's actions."[25] And researchers soon discovered "something even more distressing": contrary to its representations, "Facebook was tracking its users after they'd logged out of the site."[26]

20. In December 2007, less than a month after the Beacon's introduction, Mark Zuckerberg issued an apology, acknowledging the company "missed the right balance."[27] Moving forward, Zuckerberg said, "[i]f you select that you don't want to share some Beacon actions or if you turn off Beacon, then Facebook won't store those actions even when partners send them to Facebook."[28]

III. *LANE V. FACEBOOK*

21. In October 2008, nineteen Facebook users filed suit against Facebook and "Facebook Beacon Activated Affiliates," including Blockbuster, Fandango, and Gamefly. Facebook, they alleged, unlawfully intercepted their electronic communications, including communications that disclosed their sensitive information, like their video-viewing history, while the Facebook Beacon Activated Affiliates unlawfully permitted these disclosures.[29] This conduct,

---

[23] *Id.*
[24] Brett Winterford, *Logged in or out, Facebook is watching you*, ZDNET (Dec. 3, 2007), https://www.zdnet.com/article/logged-in-or-out-facebook-is-watching-you/.
[25] *Id.*
[26] Craig Ruttle, *Facebook CEO Apologizes, Lets Users Turn Off Beacon*, WIRED (Dec. 5, 2007), https://www.wired.com/2007/12/facebook-ceo-apologizes-lets-users-turn-off-beacon/.
[27] FACEBOOK, ANNOUNCEMENT: FACEBOOK USERS CAN NOW OPT-OUT OF BEACON FEATURE, https://about.fb.com/news/2007/12/announcement-facebook-users-can-now-opt-out-of-beacon-feature/.
[28] *Id.*
[29] *Lane v. Facebook*, 5:08-cv-03845-RS, Dkt. 1 (N.D. Cal. Aug. 12, 2008).

plaintiffs alleged, violated several privacy protections guaranteed by law, both state and federal.[30] Specifically, by intercepting their electronic communications, Facebook violated the Electronic Communications Privacy Act, and by disclosing their video-viewing history to Facebook, the Affiliates violated the Video Privacy Protection Act ("VPPA").[31]

22. The parties ultimately agreed to settle for a $9.5 million *cy pres* fund, a settlement that the district court approved and the Ninth Circuit later upheld.[32]

23. Nonetheless, after the Beacon debacle, Facebook continued to disregard user privacy, resulting in a November 2012 consent decree between the Federal Trade Commission and Facebook,[33] which the social media site violated just seven years later, entering another agreement with additional terms and a $5 billion penalty.[34] Notwithstanding the hefty fine, Facebook continues to violate that renewed consent decree, as later discussed.

24. Twelve years after the *Lane* settlement, not much has changed. Facebook's advertisers still violate the VPPA, and Facebook still facilitates those violations by intentionally wiretapping electronic communications from users and non-users alike. Then and today, Facebook never receives consent for these interceptions, instead promising users it safeguards their privacy and requires advertisers to disclose data in compliance with federal and state law.

25. Facebook has, however, made one change, a change that represents the only lesson it learned from *Lane*. Facebook originally conceived the Beacon program as "a far more transparent and personal approach"[35] to off-site tracking, contrasting it with the industry standard, where companies track users "behind the scenes, where consumers do not notice it."[36] But Facebook failed to appreciate that "[p]eople tend to strongly oppose such tracking when they know it is

---

[30] *Id.*
[31] *Id.*
[32] *Id.* at Dkt. 38.; *Lane v. Facebook*, 696 F.3d 811 (9th Cir. 2012).
[33] FEDERAL TRADE COMMISSION, FTC APPROVES FINAL SETTLEMENT WITH FACEBOOK, https://www.ftc.gov/news-events/press-releases/2012/08/ftc-approves-final-settlement-facebook.
[34] FEDERAL TRADE COMMISSION, FTC IMPOSES $5 BILLION PENALTY AND SWEEPING NEW PRIVACY RESTRICTIONS ON FACEBOOK, https://www.ftc.gov/news-events/press-releases/2019/07/ftc-imposes-5-billion-penalty-sweeping-new-privacy-restrictions.
[35] Louise Story and Brad Stone, *Facebook Retreats on Online Tracking*, N.Y. TIMES (Nov. 30, 2007), https://www.nytimes.com/2007/11/30/technology/30face.html.
[36] *Id.*

happening or discover the extent to which it is happening."[37] That sentiment was especially true for Facebook, where users chronicle their personal lives and interact with friends and family. Indeed, in a survey commissioned the same year as the Beacon program's introduction, "85% of the respondents said they rejected outright the idea that a site they value and trust should be allowed to serve up clickstream advertisements based on data from their visits to other sites."[38] Rather than address public discomfort by curbing its tracking, Facebook discarded its "transparent and personal approach," moving its tracking "behind the scenes, where consumers do not notice it." Today, as the following allegations show, Facebook continues to ubiquitously track communications, including sensitive and confidential communication, off its site. The only difference is Facebook's transparency in doing so.

26. Plaintiffs bring this complaint to pick up where *Lane* left off.

PARTIES

27. Plaintiff Starzinski is domiciled in Los Angeles, California. Plaintiff Starzinski subscribes to and frequents Paramount+ through the website paramountplus.com, which integrates the Facebook Tracking Pixel. During those visits, the Facebook Tracking Pixel tracked what he clicked on, searched for, and the videos he viewed. At all relevant times, Plaintiff Starzinski has maintained a Facebook account. When accessing and viewing content on paramountplus.com, Plaintiff Starzinski sent and received communications with Paramount. Facebook intercepted these communications, and the Facebook Tracking Pixel captured and transmitted, at a minimum, the buttons Plaintiff Starzinski clicked and the Universal Resource Locator ("URL") for the pages he viewed. While visiting paramountplus.com, Plaintiff Starzinski was unaware that Facebook was intercepting these communications in real-time, and Plaintiff Starzinski did not consent to these interceptions.

28. Plaintiff Odumosu is domiciled in Santa Clarita, California. Plaintiff Odumosu subscribes to and frequents ESPN+ and Hulu through the websites espn.com and hulu.com, which

[37] Jaikumar Vijayan and Heather Havenstein, *Facebook's Beacon just the tip of the privacy iceberg,* COMPUTERWORLD (Dec. 3, 2007), https://www.computerworld.com/article/2538002/facebook-s-beacon-just-the-tip-of-the-privacy-iceberg.html

[38] *Id.*

integrate the Facebook Tracking Pixel, and has done so many times. During those visits, the Facebook Tracking Pixel tracked what he clicked on, searched for, and the videos he viewed. At all relevant times, Plaintiff Odumusu has maintained a Facebook account. When accessing and viewing content on espn.com and hulu.com, Plaintiff Odumosu sent and received communications with ESPN and Hulu. Facebook intercepted these communications, and the Facebook Tracking Pixel captured and transmitted, at a minimum, the buttons Plaintiff Odumosu clicked and the Universal Resource Locator ("URL") for the pages he viewed. While visiting espn.com and hulu.com, Plaintiff Odumosu was unaware that Facebook was intercepting these communications in real-time, and Plaintiff Odumosu did not consent to these interceptions.

29. Plaintiff Medina is domiciled in Los Angeles, California. Plaintiff Medina subscribes to and frequents Hulu through the website hulu.com, which integrates the Facebook Tracking Pixel. During those visits, the Facebook Tracking Pixel tracked what he clicked on, searched for, and the videos he viewed. At all relevant times, Plaintiff Medina has maintained a Facebook account. When accessing and viewing content on hulu.com, Plaintiff Medina sent and received communications with Hulu. Facebook intercepted these communications, and the Facebook Tracking Pixel captured and transmitted, at a minimum, the buttons Plaintiff Medina clicked and the Universal Resource Locator ("URL") for the pages he viewed. While visiting hulu.com, Plaintiff Medina was unaware that Facebook was intercepting these communications in real-time, and Plaintiff Medina did not consent to these interceptions.

30. Plaintiff McCoy is domiciled in Manteca, California. Plaintiff McCoy subscribes to and frequents Starz through the website starz.com, which integrates the Facebook Tracking Pixel. During those visits, the Facebook Tracking Pixel tracked what he clicked on, searched for, and the videos he viewed. At all relevant times, Plaintiff McCoy has maintained a Facebook account. When accessing and viewing content on starz.com, Plaintiff McCoy sent and received communications with Starz. Facebook intercepted these communications, and the Facebook Tracking Pixel captured and transmitted, at a minimum, the buttons Plaintiff McCoy clicked and the Universal Resource Locator ("URL") for the pages he viewed. While visiting starz.com, Plaintiff

McCoy was unaware that Facebook was intercepting these communications in real-time, and Plaintiff McCoy did not consent to these interceptions.

31. Defendant Meta Platforms, Inc. is a social media site that requires users to submit their "real identity" when creating an account, meaning a first name, last name, birthday and gender. Defendant is a Delaware corporation with its principal place of business in Menlo Park, California. Defendant develops, owns, and operates facebook.com, which is used throughout California and the United States.

JURISDICTION AND VENUE

32. This Court has subject matter jurisdiction over this class action. This Court has personal jurisdiction over the parties because Plaintiffs reside in California and submit to the jurisdiction of the Court, and because Defendant, at all times relevant hereto, has systematically and continually conducted, and continues to conduct, business in this State.

33. Venue is proper in this Court pursuant to Civil Code §§ 395 and 395.5. Defendant conducts business in this County and throughout the State of California and its principal place of business is in this County.

STATEMENT OF FACTS

I. FACEBOOK'S PLATFORM AND ITS BUSINESS TOOLS

34. Facebook describes itself as a "real identity platform,"[39] meaning users are allowed only one account and must share "the name they go by in everyday life."[40] To that end, when creating an account, users must provide their first and last name, along with their birthday and gender.[41]

35. In 2021, Facebook generated $117 billion in revenue.[42] Roughly 97% of that came

[39] Sam Schechner and Jeff Horwitz, *How Many Users Does Facebook Have? The Company Struggles to Figure It Out*, WALL. ST. J. (Oct. 21, 2021).
[40] FACEBOOK, COMMUNITY STANDARDS, PART IV INTEGRITY AND AUTHENTICITY, https://www.facebook.com/communitystandards/integrity_authenticity.
[41] FACEBOOK, SIGN UP, https://www.facebook.com/
[42] FACEBOOK, META REPORTS FOURTH QUARTER AND FULL YEAR 2021 RESULTS, https://investor.fb.com/investor-news/press-release-details/2022/Meta-Reports-Fourth-Quarter-and-Full-Year-2021-Results/default.aspx

from selling advertising space.[43]

36. Facebook sells advertising space by highlighting its ability to target users.[44] Facebook can target users so effectively because it surveils user activity both on and off its site.[45] This allows Facebook to make inferences about users beyond what they explicitly disclose, like their "interests," "behavior," and "connections."[46] Facebook compiles this information into a generalized dataset called "Core Audiences," which advertisers use to apply highly specific filters and parameters for their targeted advertisements.[47]

37. Advertisers can also build "Custom Audiences."[48] Custom Audiences enables advertisers to reach "people who have already shown interest in [their] business, whether they're loyal customers or people who have used [their] app or visited [their] website."[49] With Custom Audiences, advertisers can target existing customers directly, and they can also build a "Lookalike Audiences," which "leverages information such as demographics, interests, and behavior from your source audience to find new people who share similar qualities."[50] Unlike Core Audiences, advertisers can build Custom Audiences and Lookalike Audiences only if they first supply Facebook with the underlying data. They can do so through two mechanisms: by manually uploading contact information for customers, or by utilizing Facebook's "Business Tools."[51]

---

[43] *Id.*

[44] FACEBOOK, WHY ADVERTISE ON FACEBOOK, https://www.facebook.com/business/help/205029060038706.

[45] FACEBOOK, ABOUT FACEBOOK PIXEL, https://www.facebook.com/business/help/742478679120153?id=1205376682832142.

[46] FACEBOOK, AD TARGETING: HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[47] FACEBOOK, EASIER, MORE EFFECTIVE WAYS TO REACH THE RIGHT PEOPLE ON FACEBOOK, https://www.facebook.com/business/news/Core-Audiences.

[48] FACEBOOK, ABOUT CUSTOM AUDIENCES, https://www.facebook.com/business/help/744354708981227?id=2469097953376494.

[49] FACEBOOK, AD TARGETING, HELP YOUR ADS FIND THE PEOPLE WHO WILL LOVE YOUR BUSINESS, https://www.facebook.com/business/ads/ad-targeting.

[50] Facebook, About Lookalike Audiences, https://www.facebook.com/business/help/164749007013531?id=401668390442328.

[51] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494; Facebook, Create a Website Custom Audience, https://www.facebook.com/business/help/1474662202748341?id=2469097953376494.

II. FACEBOOK UTILIZES ITS BUSINESS TOOLS TO INTENTIONALLY INTERCEPT ELECTRONIC COMMUNICATIONS

38. As Facebook puts it, the Business Tools "help website owners and publishers, app developers and business partners, including advertisers and others, integrate with Facebook, understand and measure their products and services, and better reach and serve people who might be interested in their products and services."[52] Put more succinctly, Facebook's Business Tools are bits of code that advertisers can integrate into their website, mobile applications, and servers, thereby enabling Facebook to intercept and collect user activity on those platforms.

39. The Business Tools are automatically configured to capture certain data, like when a user visits a webpage, that webpage's Universal Resource Locator ("URL") and metadata, or when a user downloads a mobile application or makes a purchase.[53] Facebook's Business Tools can also track other events. Facebook offers a menu of "standard events" from which advertisers can choose, including what content a visitor views or purchases.[54] Advertisers can even create their own tracking parameters by building a "custom event."[55]

40. One such Business Tool is the Facebook Tracking Pixel. Facebook offers this piece of code to advertisers, including each of the Streaming Services, to integrate into their respective websites. As the name implies, the Facebook Tracking Pixel "tracks the people and type of actions they take."[56] When a user accesses a website hosting the Facebook Tracking Pixel, Facebook's software script surreptitiously directs the user's browser to send a separate message to Facebook's servers. This second, secret transmission contains the original GET request sent to the host website, along with additional data that the Pixel is configured to collect. This transmission is initiated by

---

[52] FACEBOOK, THE FACEBOOK BUSINESS TOOLS, https://www.facebook.com/help/331509497253087.
[53] *See* FACEBOOK, FACEBOOK PIXEL, ACCURATE EVENT TRACKING, ADVANCED, https://developers.facebook.com/docs/facebook-pixel/advanced/; *see also* FACEBOOK, BEST PRACTICES FOR FACEBOOK PIXEL SETUP, https://www.facebook.com/business/help/218844828315224?id=1205376682832142; FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.
[54] FACEBOOK, SPECIFICATIONS FOR FACEBOOK PIXEL STANDARD EVENTS, https://www.facebook.com/business/help/402791146561655?id=1205376682832142.
[55] FACEBOOK, ABOUT STANDARD AND CUSTOM WEBSITE EVENTS, https://www.facebook.com/business/help/964258670337005?id=1205376682832142; *see also* FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/.
[56] FACEBOOK, RETARGETING, https://www.facebook.com/business/goals/retargeting.

Facebook's code and concurrent with the communications with the host website. Two sets of code are thus automatically run as part of the browser's attempt to load and a website—the website's own code, and Facebook's embedded code.

41. After collecting and intercepting this information, Facebook processes it, analyzes it, and assimilates it into datasets like Core Audiences and Custom Audiences.

42. Facebook's other Business Tools function the same. For mobile applications, advertisers can utilize the Facebook SDK, which contains "component SDKs," like the App Events API, allowing advertisers to track events on their mobile apps so they can "measure ad performance and build audiences for ad targeting."[57]

43. Advertisers can also utilize the "Conversions API." The Conversions API lets advertisers circumvent a user's choice to exercise privacy controls.[58] More technically, the Conversions API is Facebook code that advertisers can implement server-side.[59] Because it operates server-side, the Conversions API ignores users' decision to opt out of tracking, collecting the same data it would otherwise through "a connection between an advertiser's server and Facebook."[60] When the Conversions API collects "[s]erver events," those data points are "linked to a Meta Pixel ID and are processed like web events sent via Pixel."[61] As with the Facebook Tracking Pixel, the Conversions API intercepts these communications contemporaneously and surreptitiously.[62] Facebook "recommend[s] that advertisers implement the Conversions API alongside their Meta Pixel and follow other best practices."[63]

44. Facebook intercepted Plaintiffs' electronic communications each time they accessed

---

[57] FACEBOOK, APP EVENTS API, https://developers.facebook.com/docs/marketing-api/app-event-api/

[58] FACEBOOK, CONVERSIONS API, https://developers.facebook.com/docs/marketing-api/conversions-api. This refers to device specific privacy controls.

[59] *Id.*

[60] *Id.*

[61] *Id.*

[62] FACEBOOK, HANDLING DUPLICATE PIXEL AND CONVERSIONS API EVENTS, https://developers.facebook.com/docs/marketing-api/conversions-api/deduplicate-pixel-and-server-events/ ("Once your event fulfills both conditions, we keep the first one and remove the following one. If a server and browser event arrive at approximately the same time (within 15 seconds of each other), we favor the browser event.").

[63] *Id.*

a website containing the Facebook Tracking Pixel, like the Streaming Services' websites. Facebook intercepted these communications even when they were confidential and sensitive, like when a subscriber ordered video material from the Streaming Services.

III. FACEBOOK UTILIZES ITS BUSINESS TOOLS TO INTENTIONALLY INTERCEPT SENSITIVE AND CONFIDENTIAL COMMUNICATIONS

45. The Streaming Services coordinate with Facebook to target their advertisements and set up their Business Tools. Facebook's "Solutions Engineers team," a team with more than 100 employees, "works with advertisers to build the technology and infrastructure needed to run more effective campaigns on Facebook, often on top of Facebook's APIs."[64] This team and others work with the Streaming Services closely.

46. For its top spenders, Facebook also embeds employees to provide strategic advice. This is confirmed through Facebook's own acknowledgements and congressional testimony. During the 2016 presidential race, Facebook helped campaigns with their digital outreach, providing a "political ad strategy [that] was initially modeled on its playbook for top corporate clients: Facebook employees offered on-site support to the U.S. presidential candidates who were considered the presumptive nominees for their parties."[65] When called before Congress to explain the practice, Facebook supplied written answers reiterating its approach was "consistent with support provided to commercial clients in the normal course of business."[66] As top corporate clients, Facebook provides the Streaming Services with this same level of support, helping the Streaming Services to, among other things, set up and maximize Facebook's Business Tools.

A. The Streaming Services and Facebook's Business Tools

47. To target its ads, the Streaming Services use Facebook's Business Tools. These

---

[64] Anthony Ha, *Facebook has a 100-person engineering team that helps advertisers build tools and infrastructure*, TECHCRUNCH (Dec. 29, 2017), https://techcrunch.com/2017/12/29/facebook-solutions-engineering/.

[65] Deepa Seetharaman, *How a Facebook Employee Helped Trump Win—But Switched Sides for 2020*, WALL ST. J. (Nov. 24, 2019), https://www.wsj.com/articles/how-facebooks-embed-in-the-trump-campaign-helped-the-president-win-11574521712.

[66] ENERGY AND COMMERCE COMMITTEE, APRIL 11, 2018 HEARING TITLED FACEBOOK: TRANSPARENCY AND USE OF CONSUMER DATA, https://energycommerce.house.gov/sites/democrats.energycommerce.house.gov/files/documents/House%20QFRs.compressed.pdf.

include, at a minimum, the Facebook Tracking Pixel and Facebook's SDK.

48. For example, the Streaming Services' websites each host the Facebook Tracking Pixel and transmit PageView data to Facebook, which includes the Uniform Resource Locators ("URL") dedicated solely to the specific video watched.

49. This event data permits an ordinary person to identify what video(s) an individual has watched, and transmits this information in real time.

50. For example, Espn.com contains the code for at least ten different Facebook cookies:

Name	Value	Domain
fr	1Q1mbbo0rSihNtl0...	.facebook.com
xs	35%3ADindSa0sHK...	.facebook.com
locale	en_US	.facebook.com
ps_l	1	.facebook.com
datr	YmzSZBe2c5VKjUNs...	.facebook.com
c_user	[redacted]	.facebook.com
presence	C%7B%22t3%22%3...	.facebook.com
wd	1753x832	.facebook.com
ps_n	1	.facebook.com
sb	f2jBZbzuD_4mOqP3...	.facebook.com

51. Hulu.com contains the code for at least 10 different Facebook cookies:

Name	Value	Domain
c_user	[redacted]	.facebook.com
datr	YmzSZBe2c5VKjUNs...	.facebook.com
fr	1U9Vq1LmJpivOrcG...	.facebook.com
locale	en_US	.facebook.com
presence	C%7B%22t3%22%3...	.facebook.com
ps_l	1	.facebook.com
ps_n	1	.facebook.com
sb	f2jBZbzuD_4mOgP3...	.facebook.com
wd	1854x855	.facebook.com
xs	35%3ADindSa0sHK...	.facebook.com

52. Paramountplus.com contains the code for at least seven different Facebook cookies:

Name	Value	Domain
sb	jVa6YaHou2Nev98LS...	.facebook.com
fr	1ey4SzLZuxHSXJ3y8....	.facebook.com
xs	165%3AjYP2J9Bb8vt...	.facebook.com
ps_l	1	.facebook.com
c_user	[redacted]	.facebook.com
ps_n	1	.facebook.com
datr	D8aAZZE7dAvjNYke...	.facebook.com

53. Starz.com contains the code for at least ten different Facebook cookies:

Name	Value	Domain
c_user	[redacted]	.facebook.com
datr	YmzSZBe2c5VKjUNs...	.facebook.com
fr	1U9Vq1LmJpivOrcG...	.facebook.com
locale	en_US	.facebook.com
presence	C%7B%22t3%22%3...	.facebook.com
ps_l	1	.facebook.com
ps_n	1	.facebook.com
sb	f2jBZbzuD_4mOgP3...	.facebook.com
wd	1854x855	.facebook.com
xs	35%3ADindSa0sHK...	.facebook.com

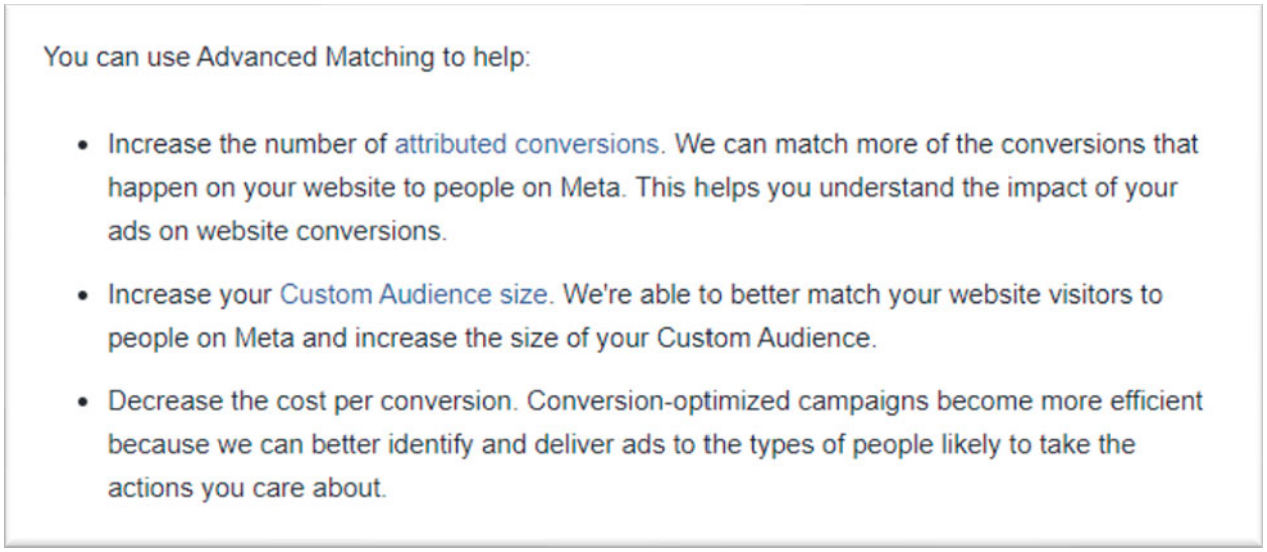
B. The Facebook Tracking Pixel Matches the Content to a Subscriber's Identity

54. The Facebook Tracking Pixel matches Streaming Services subscribers to their corresponding Facebook profiles.

55. The Streaming Services' Facebook Tracking Pixels utilize "Automatic Advanced Matching." Automatic Advanced Matching enables a Facebook Tracking Pixel to "look for recognizable form field and other sources on your website that contain information such as first name, last name and email."[67] The Facebook Tracking Pixel's code then intercepts and transmits that information, "along with the event, or action, that took place."[68] This information is

[67] FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB, https://www.facebook.com/business/help/611774685654668?id=1205376682832142
[68] *Id.*

"hashed,"[69] meaning it is "[a] computed summary of digital data that is a one-way process."[70]



You can use Advanced Matching to help:

- Increase the number of attributed conversions. We can match more of the conversions that happen on your website to people on Meta. This helps you understand the impact of your ads on website conversions.
- Increase your Custom Audience size. We're able to better match your website visitors to people on Meta and increase the size of your Custom Audience.
- Decrease the cost per conversion. Conversion-optimized campaigns become more efficient because we can better identify and deliver ads to the types of people likely to take the actions you care about.

56. In other words, it "cannot be reversed back into the original data."[71]

57. Facebook intercepts and collects this information so it can better match visitors to their Facebook profiles, which in turn allows the Streaming Services to better target their advertisements.[72]

58. Facebook intercepts and collects this information notwithstanding whether a user is logged into Facebook or has ever registered for an account.

59. Facebook also uses various cookies to supplement the Facebook Tracking Pixel's tracking practices. Specifically, the Facebook Tracking Pixel contains a script that causes the user's browser to transmit, to Facebook, information from each of the Facebook cookies already existing on the browser's cache.

60. A subscriber who watches a show on the Streaming Services while logged into

[69] PCMAG ENCYCLOPEDIA, HASH, https://www.pcmag.com/encyclopedia/term/hash.
[70] *Id.*
[71] *Id.*
[72] FACEBOOK, ABOUT ADVANCED MATCHING FOR WEB, https://www.facebook.com/business/help/611774685654668?id=1205376682832142

Facebook transmits the c_user cookie to Facebook, which contains that subscriber's unencrypted Facebook ID.

61. When a visitor's browser has recently logged out of an account, Facebook compels the visitor's browser to send a smaller set of cookies.

62. The fr cookie contains, at least, an encrypted Facebook ID and browser identifier.[73] The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser.[74] The datr cookies also identifies a browser. Facebook, at a minimum, uses the fr and _fbp cookies to identify users.[75]

63. Without a corresponding Facebook ID, the fr cookie contains, at least, an abbreviated and encrypted value that identifies the browser. The _fbp cookie contains, at least, an unencrypted value that uniquely identifies a browser. Facebook uses both for targeted advertising.

64. The fr cookie expires after 90 days unless the visitor's browser logs back into Facebook.[76] If that happens, the time resets, and another 90 days begins to accrue.[77]

65. The _fbp cookie expires after 90 days unless the visitor's browser accesses the same website.[78] If that happens, the time resets, and another 90 days begins to accrue.[79]

66. The Facebook Tracking Pixel uses both first- and third-party cookies. A first-party cookie is "created by the website the user is visiting"—*i.e.*, the Streaming Services.[80] A third-party cookie is "created by a website with a domain name other than the one the user is currently

---

[73] DATA PROTECTION COMMISSIONER, FACEBOOK IRELAND LTD, REPORT OF RE-AUDIT (Sept. 21, 2012), http://www.europe-v-facebook.org/ODPC_Review.pdf.

[74] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[75] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[76] *See* FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[77] Confirmable through developer tools.

[78] *See* FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policy/cookies/.

[79] Also confirmable through developer tools.

[80] PC MAG, FIRST-PARTY COOKIES, https://www.pcmag.com/encyclopedia/term/first-party-cookie. This is confirmable by using developer tools to inspect a website's cookies and track network activity.

visiting"—*i.e.*, Facebook.[81] The _fbp cookie is always transmitted as a first-party cookie. A duplicate _fbp cookie is sometimes sent as a third-party cookie, depending on whether the browser has recently logged into Facebook.

67. Facebook, at a minimum, uses the fr, _fbp, and c_user cookies to link to Facebook IDs and corresponding Facebook profiles.

68. A Facebook ID is personally identifiable information. Anyone can identify a Facebook profile—and all personal information publicly listed on that profile—by appending the Facebook ID to the end of Facebook.com.

69. Facebook links these identifiers with the event data, allowing Facebook to know, among other things, which videos a subscriber has watched through the Streaming Services.[82]

70. By compelling a visitor's browser to transmit the Advanced Matching parameters alongside event data for videos, Facebook intentionally intercepted electronic communications that Plaintiffs and Class members sent and received while viewing videos on the Streaming Services' platforms. Because the communications contained personally identifiable information—information that numerous federal and state laws recognize as protected and sensitive—Facebook intercepted confidential communications.

71. By compelling a visitor's browser to transmit the c_user cookie alongside event data for videos, Facebook intentionally intercepted electronic communications that Plaintiffs and Class members sent and received while viewing videos on the Streaming Services' platforms. Because the communications contained personally identifiable information—information that numerous federal and state laws recognize as protected and sensitive—Facebook intercepted confidential communications.

72. By compelling a visitor's browser to transmit the fr and _fbp cookie alongside event data for videos, Facebook intentionally intercepted electronic communications that Plaintiffs and Class members sent and received while viewing videos on the Streaming Services' platforms.

---

[81] PC MAG, THIRD-PARTY COOKIES, https://www.pcmag.com/encyclopedia/term/third-party-cookie. This is also confirmable by tracking network activity.

[82] FACEBOOK, GET STARTED, https://developers.facebook.com/docs/meta-pixel/get-started.

Because the communications contained personally identifiable information—information that numerous federal and state laws recognize as protected and sensitive—Facebook intercepted confidential communications.

73. By compelling a visitor's browser to disclose the fr cookie and other browser identifiers alongside event data for videos, Facebook intentionally intercepted electronic communications that Plaintiffs and Class members sent and received while viewing videos on the Streaming Services' platforms. Because the communications contained personally identifiable information—information that numerous federal and state laws recognize as protected and sensitive—Facebook intercepted confidential communications.

74. By utilizing its other Business Tools to compel disclosure of identifiers alongside event data for videos, Facebook intentionally intercepted electronic communications that Plaintiffs and Class members sent and received while viewing videos on the Streaming Services' platforms. Because the communications contained personally identifiable information—information that numerous federal and state laws recognize as protected and sensitive—Facebook intercepted confidential communications.

C. The Facebook Tracking Pixel Matches the Content to a Subscriber's Identity

75. The origins of the VPPA begin with President Ronald Reagan's nomination of Judge Robert Bork to the United States Supreme Court. During the confirmation process, a movie rental store disclosed the nominee's rental history to the Washington City Paper, who then published that history. Congress responded by passing the VPPA, with an eye toward the digital future. As Senator Patrick Leahy, who introduced the Act, explained:

> It is nobody's business what Oliver North or Robert Bork or Griffin Bell or Pat Leahy watch on television or read or think about when they are home. In an area of interactive television cables, the growth of computer checking and check-out counters, of security systems and telephones, all lodged together in computers, it would be relatively easy at some point to give a profile of a person and tell what they buy in a store, what kind of food they like, what sort of television programs they watch, who are some of the people they telephone. I think that is wrong.

S. Rep. 100-599, at 5-6 (internal ellipses and brackets omitted).

76. The VPPA prohibits "[a] video tape service provider who knowingly discloses, to any person, personally identifiable information concerning any consumer of such provider." 18 U.S.C. § 2710(b)(1). The VPPA defines personally identifiable information as "information which identifies a person as having requested or obtained specific video materials or services from a video service provider." 18 U.S.C. § 2710(a)(3). A video tape service provider is "any person, engaged in the business, in or affecting interstate or foreign commerce, of rental, sale, or delivery of prerecorded video cassette tapes or similar audio visual materials." 18 U.S.C. § 2710(a)(4).

77. The Streaming Services, along with Facebook, knowingly violate the Video Privacy Protection Act. The Streaming Services have a singular purpose: the "delivery of prerecorded video cassette tapes or similar audio visual material." 18 U.S.C. § 2710(b)(4). To access the Streaming Services' content, viewers must pay money on a recurring basis, making them subscribers and therefore consumers. 18 U.S.C. § 2710(a)(1). The Streaming Services utilize the Business Tools to provide Facebook with "information which identifies a person as having requested or obtained specific materials or services," from the Streaming Services themselves. 18 U.S.C. § 2710(a)(3). Because these tools only serve to sell advertising space and target advertisements, Facebook never engages in "debt collection activities, order fulfillment, request processing, [or] the transfer of ownership." 18 U.S.C. § 2710(a)(2). And the Streaming Services fail to include any terms, let alone terms "in a form distinct and separate" from other legal obligations, that come close to satisfying the VPPA's consent requirements. Under even a generous reading of the VPPA, the Streaming Services flagrantly violate federal and state privacy laws.

78. Along with being unlawfully disclosed, a subscriber's video-viewing history also constitutes sensitive information. Plaintiffs and the Class members have a cognizable interest in keeping detailed data about what video content they watch private. This is evinced by, among other things, the various federal and state statutes—including a California statute—that specifically protect video viewing histories. *See, e.g.*, Cal. Civ. Code § 1799.3 ("No person providing video recording sales or rental services shall disclose any personal information or the contents of any record, including sales or rental information, which is prepared or maintained by that person, to any person, other than the individual who is subject of the record, without the written consent of that

individual.").

79. Similarly, subscribers' communications with the Streaming Services were confidential. Subscribers had the reasonable expectation that no third parties would eavesdrop on their protected communications with the Streaming Services.

80. Plaintiffs' and Class members' expectation of privacy was reasonable, not only because of Facebook's various representations, but also because of survey data showing the expectations of Internet users. A number of studies examining the collection of consumers' personal data confirms that the surreptitious taking of personal, confidential, and private information—as Facebook has done—violates reasonable expectations of privacy that have been established as general social norms. Privacy polls and studies uniformly show that the overwhelming majority of Americans consider one of the most important privacy rights to be the need for an individual's affirmative consent before a company collects and shares a subscriber's personal data. Indeed, a recent study by Consumer Reports shows that 92% of Americans believe that internet companies and websites should be required to provide consumers with a complete list of the data that has been collected about them.[83]

81. Likewise, a study published in the *Harvard Business Review* shows that consumers are largely unaware of how their personal information is used by businesses, with less than 25% of consumers realizing that they share their communication history, IP addresses, and web-surfing history when using a standard web browser.[84] It is also common sense that Facebook should not intercept or collect user communications when users are transmitting protected information, like their video-viewing history.

82. Moreover, since 2018, states like California passed the CCPA, which requires that data collection practices be disclosed at or before the actual collection is done. Otherwise, "[a] business shall not collect additional categories of personal information or use personal information

[83] *Consumers Less Confident About Healthcare, Data Privacy, and Car Safety, New Survey Finds*, CONSUMER REPORTS (May 11, 2017), https://www.consumerreports.org/consumer-reports/consumers-less-confident-about-healthcare-data-privacy-and-car-safety-a3980496907/.

[84] Timothy Morey, Theodore Forbath & Allison Shoop, *Customer Data: Designing for Transparency and Trust,* HARV. BUS. REV. (May 2015), https://hbr.org/2015/05/customer-data-designing-for-transparency-and-trust.

collected for additional purposes without providing the consumers with notice consistent with this section." Cal. Civ. Code § 1798.100(b).

83. By collecting intimate, sensitive, and confidential communications, Facebook also committed a highly offensive intrusion, especially when considering the quantum and nature of the information collected, Facebook's failure to respect consumers' privacy choices, and the divergence from the standard industry practice, which is to keep those communications confidential.

84. Facebook knows that it intercepted sensitive and unlawfully disclosed information that the Streaming Services had no legal right to transmit. This conclusion is inescapable given Facebook's own history with the VPPA, its partnership with the Streaming Services, and the amount of money the Streaming Services spend on advertisements.

IV. FACEBOOK NEVER RECIEVES CONSENT TO INTENTIONALLY INTERCEPT CONFIDENTIAL AND SENSITIVE INFORMATION

A. Facebook's Terms of Service, Cookies Policy, and Data Policy

85. Facebook never receives consent from users to intercept and collect electronic communications containing their sensitive and unlawfully-disclosed information. In fact, Facebook expressly warrants the opposite.

86. When first signing up, a user assents to three agreements: the Terms of Service,[85] the Cookies Policy,[86] and the Data Policy.[87] For California residents, Facebook also publishes a California Privacy Policy.[88]

87. Facebook's Terms of Service begins by stating that "[p]rotecting people's privacy is central to how we've designed our ad system."[89] The Terms of Service then prohibits anyone from using Facebook's Products in a manner that is "unlawful, misleading, discriminatory or fraudulent."[90]

88. Facebook's Data Policy recognizes that there may be "[d]ata with special

[85] FACEBOOK, TERMS OF SERVICE, https://www.facebook.com/legal/terms/update.
[86] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies/.
[87] FACEBOOK, DATA POLICY, https://www.facebook.com/about/privacy/update.
[88] FACEBOOK, CALIFORNIA PRIVACY NOTICE, https://www.facebook.com/legal/policy/ccpa.
[89] FACEBOOK, TERMS OF SERVICE, https://www.facebook.com/legal/terms/update..
[90] *Id.*

protections," meaning information that "could be subject to special protections under the laws of your country."[91] The Data Policy goes on to describe how Facebook collects information from its "Meta Business Tools," including "our social plug-ins (such as the Like button), Facebook Login, our APIs and SDKs, or the Meta pixel."[92] Specifically, Facebook acknowledges that "[p]artners receive your data when you visit or use their services or through third parties they work with."[93]

89. Facebook then offers an express representation: "**We require each of these partners to have lawful rights to collect, use and share your data before providing any data to us**."[94] Facebook does acknowledge collecting "data with special protections" to personalize ads, but critically, only sensitive information that users "choose to provide."[95]

90. Facebook's Cookies Policy ratifies those representations, stating "the Data Policy will apply to our processing of the data that we collect via cookies."[96]

91. For California residents, Facebook reiterates that policy: "We require each of these partners to have rights to collect, use, and share your data before providing any data to us."[97] The California Privacy Policy also restrict Facebook's ability to collect "data with special protections," stating they do so only when users "choose to provide it."[98]

92. Facebook intentionally intercepts sensitive and unlawfully disclosed information and knowingly facilitates an advertiser's violation of state and federal privacy law. That is enough to show that Facebook violates its Terms of Service, Data Policy, Cookies Policy, and California Privacy Policy. Facebook is no mere passive conduit to the Streaming Services' unlawful conduct. Facebook aids and abets the Streaming Services' disclosure of personally identifiable information, then profits from it. As one of the largest spenders on Facebook advertising, Facebook helps the Streaming Services configure and set up their Business Tools. Facebook also helps the Streaming

---

[91] FACEBOOK, DATA POLICY, https://www.facebook.com/about/privacy/update.
[92] FACEBOOK, DATA POLICY, https://www.facebook.com/about/privacy/update.
[93] *Id.*
[94] *Id.*
[95] *Id.*
[96] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies/.
[97] FACEBOOK, CALIFORNIA PRIVACY NOTICE, https://www.facebook.com/legal/policy/ccpa.
[98] *Id.*

Services strategize on how to distribute the part of their advertising budget apportioned for the social media site, which totals millions of dollars annually. Rather than "require each of these partners to have the rights to collect, use and share your data," Facebook aids and abets a knowing violation of federal and state laws.

93. At a minimum, Facebook knows the Streaming Services unlawfully disclose their subscribers' personally identifiable information. The Streaming Services are among the largest subscription-based video providers in the country and spend millions of dollars annually on Facebook's targeted advertisements. The social media site must process those payments, analyze the Streaming Services' data, assimilate that data into the Streaming Services' Custom Audiences, and incorporate it into Core Audiences. Given the scale and persistence of these disclosures, the only reasonable conclusion is that Facebook knows the Streaming Services disclose personally identifiable information, a disclosure that the Streaming Services have no lawful right to make. Users never choose to provide this sensitive information to Facebook because, among other reasons, they never know whether a particular website uses its Business Tools, and, if so, what data those tools collect.

B. Facebook's Other Representations

94. Facebook's other representations reinforce these warranties. In its Advertising Policy, Facebook states "[w]e do not use sensitive personal data for ad targeting."[99] And in a blog post titled "About Restricted Meta Business Tools Data," Facebook asserts it has "policies around the kinds of information businesses can share with us."[100] Facebook does not "want websites or apps sending us sensitive information about people."[101] Sensitive information includes, among other things, "any information defined as sensitive under applicable laws, regulations and applicable industry guidelines."[102]

95. These representations are repeated frequently. Facebook created a "Help Center" to

[99] FACEBOOK, ADVERTISING POLICY, https://www.facebook.com/policies/ads/.
[100] FACEBOOK, ABOUT RESTRICTED META BUSINESS TOOLS DATA, https://www.facebook.com/business/help/1057016521436966?id=188852726110565
[101] *Id.*
[102] *Id.*

better explain its practices to users. In an article titled, "How does Facebook receive information from other businesses and organizations?," Facebook reiterates its promise to "prohibit businesses or organizations from sharing sensitive information with us," and if Facebook "determine[s] that a business or an organization is violating our terms, we'll take action against that business or organization."[103] In another article, titled, "How does Meta work with data providers?," Facebook repeats this promise, stating "[b]usinesses that advertise on Facebook are required to have any necessary rights and permissions to use this information, as outlined in our Custom Audience Terms that businesses must agree to."[104]

96. But by facilitating the Streaming Services' unlawful disclosure of sensitive information, Facebook fails to uphold this promise, a failure that also extends to other forms of sensitive information. A recent Wall Street Journal investigation, for example, found that "[t]he social-media giant collects intensely personal information from many popular smartphone apps just seconds after users enter it, even if the user has no connection to Facebook, according to testing done by The Wall Street Journal."[105] The investigation focused on "analytics tools Facebook offers developers, which allows them to see statistics about their users' activities—and to target those users with Facebook ads."[106] That capability, the investigation noted, "is partly why Facebook's revenue is soaring."[107]

97. The investigation prompted the New York State Department of Financial Services to initiate its own investigation, authoring an analysis titled, "Report on Investigation of Facebook Inc. Data Privacy Concerns."[108] That report concluded:

---

[103] FACEBOOK, HOW DOES FACEBOOK RECEIVE INFORMATION FROM OTHER BUSINESSES AND ORGANIZATIONS, https://www.facebook.com/help/2230503797265156.

[104] HOW DOES META WORK WITH DATA PROVIDERS?, https://www.facebook.com/help/494750870625830?ref=dp.

[105] Sam Schechner and Mark Secada, *You Give Apps Sensitive Personal Information. Then They Tell Facebook*, WALL ST. J. (Feb. 22, 2019), https://www.wsj.com/articles/you-give-apps-sensitive-personal-information-then-they-tell-facebook-11550851636.

[106] *Id*.

[107] *Id*.

[108] NEW YORK STATE DEPARTMENT OF FINANCE, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

> [T]he sharing of sensitive user information by an app developer is a violation of Facebook Business Tools' terms of service. Merely stating a rule, however, has little meaning if the rule is not enforced, and the unfortunate fact is that Facebook does little to track whether app developers are violating this rule and takes no real action against developers that do. … Until there are real ramifications for violating Facebook's policies, Facebook will not be able to effectively prohibit the sharing of sensitive user data with third parties.[109]

98. the Streaming Services' disclosures continue unabated because Facebook fails to meaningfully require video service providers to protect a subscriber's personally identifiable information.

99. A reasonable user who reads Facebook's terms and representations would understand those terms as requiring Facebook to enforce an advertiser's compliance with its terms. At a minimum, those terms and representations require Facebook to build minimum safeguards for sensitive information, like a subscriber's personally identifiable information. No reasonable user would read those terms and representations as permitting Facebook to intentionally intercept electronic communications that it knows the law protects and deems sensitive. And no user, reasonable or not, could read those terms as allowing Facebook to aid and abet another party's disclosure of such protected and sensitive information. In short, Facebook never receives consent from users to intentionally intercept and monetize electronic communications disclosing sensitive information that the law protects.

V. FACEBOOK NEVER RECIEVES CONSENT TO GENERALLY INTERCEPT ELECTRONIC COMMUNICATIONS BECAUSE IT OBFUSCATES THE VOLUME, SPECIFICITY, AND TYPE OF DATA IT COLLECTS

100. For all electronic communications, Facebook still fails to receive informed consent from users because it obfuscates the volume, specificity, and type of data it collects.

[109] NEW YORK STATE DEPARTMENT OF FINANCE, REPORT ON INVESTIGATION OF FACEBOOK INC. DATA PRIVACY CONCERNS, https://www.dfs.ny.gov/system/files/documents/2021/02/facebook_report_20210218.pdf

101. Facebook offers a feature it calls "Off-Facebook activity," a report that ostensibly shows "a summary of activity that businesses and organizations share with us about your interactions with them, such as visiting their apps and websites."[110]

102. The report does provide some information. The report shows, for instance, that Facebook intercepted Plaintiffs communications with the Streaming Services.

103. Within the reports is each respective Plaintiffs' Pixel ID, which uniquely identifies each Pixel. In practice, this means each website's Facebook Tracking Pixel has a Pixel ID that differs from all other websites.[111]

104. Facebook has repeatedly said that the report shows "a summary of your activity that we receive from businesses or organizations, which includes your activity on other apps and websites."[112]

105. Commentators and users bought into that description. For example, shortly after the report's introduction, a columnist for the Washington Post said it "offers an opportunity to see in ugly detail how Facebook's advertising surveillance system actually works."[113] Another article called it a tool that "lets you see and control data that apps and websites share with the platform—and monitor the kind of information third-party apps can access."[114]

106. But the Off-Facebook Activity report only provides a selective glance at the data Facebook collects—a deceptive and misleading glance at that.

107. Facebook partially acknowledges the report's incompleteness. In an article titled, "What is off-Facebook Activity?," Facebook clarifies that it "receive[s] more details and activity

---

[110] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies/.

[111] FACEBOOK, GET STARTED, https://developers.facebook.com/docs/meta-pixel/get-started

[112] FACEBOOK, WHAT IS OFF-FACEBOOK ACTIVITY?, https://www.facebook.com/help/2207256696182627; FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies/.

[113] Geoffrey A. Fowler, *Facebook will now show you exactly how it stalks you – even when you're not using Facebook*, WASH. POST (Jan. 28, 2020), https://www.washingtonpost.com/technology/2020/01/28/off-facebook-activity-page/.

[114] Katie Teague, *Take control of your privacy online with the Off-Facebook Activity tool*, CNET (Nov. 15, 2021), https://www.cnet.com/tech/services-and-software/take-control-of-your-privacy-online-with-the-off-facebook-activity-tool/.

than what appears in your off-Facebook activity."[115] Specifically, the report omits "information [Facebook] received when you're not logged into Facebook, or when we can't confirm that you've previously used Facebook on that device."[116] In other words, the report only contains event data that is transmitted alongside a c_user cookie. Every other identifier—from Advanced Matching Parameters to the fr cookie—does not show. Facebook explains this discrepancy by citing "technical and accuracy reasons."[117]

108. But this partial acknowledgement is not a truthful one, with Facebook's existing capabilities belying that explanation. When advertisers integrate the Conversions API, for example, Facebook offers an "Event Match Score" that "indicates how effective your server event's customer information parameters may be at matching it to a Meta account."[118] These parameters are the exact same as those sent through Advanced Matching. The Event Match Score is measured "from 1 to 10," with Facebook recommending an advertiser "[a]im for an Event Match Quality score of 6.0 or higher."[119] Facebook offers this tool commercially, and it is meant to provide advertisers with accurate data. But rather than apply that same tool, or build a similar one, for its Off-Facebook Activity report, Facebook only displays data the company collects while a user is logged in. Any other activity—even when sent with the same parameters measured by the Event Match Score—never makes it into the report, including when Facebook has already matched those identifiers for an advertiser's Custom Audiences. Given Facebook's capabilities, no such "technical and accuracy reasons" can explain this shortcoming. Facebook omits this information because it seeks to obfuscate the volume of information it collects.

109. Facebook also obfuscates the specificity of the information it collects. Facebook offers a developer tool that lets advertisers receive a real-time and granular look at what data

---

[115] FACEBOOK, WHAT IS OFF-FACEBOOK ACTIVITY?, https://www.facebook.com/help/2207256696182627.
[116] FACEBOOK, WHAT IS OFF-FACEBOOK ACTIVITY?, https://www.facebook.com/help/2207256696182627.
[117] *Id.*
[118] FACEBOOK, BEST PRACTICES FOR CONVERSIONS API, https://www.facebook.com/business/help/308855623839366?id=818859032317965
[119] *Id.*

Facebook intercepts. The allegations above rely in part on that developer tool. The tool helps developers troubleshoot the Facebook Tracking Pixel, and as a consequence, its fundamental purpose is to be a reliable measurement. For the Streaming Services, for example, the tool shows the communications Facebook intercepts, identifying with particularity, for instance, a specific video watched. Plaintiffs' Off-Facebook Activity, however, only shows Facebook received a "custom" event.[120] This supplies less information than the Beacon published publicly,[121] and it is a level of ambiguity that applies consistently across the Off-Facebook Activity report. Facebook could build a tool, like it does for the Streaming Services, that records these categories of information. Facebook could, if privacy were a concern, disclose only the categories of information collected, not the content. But Facebook instead provides descriptions that are empty and generalized. As opposed to "technical and accuracy reasons," Facebook omits this information to mislead users and the public from the true extent of its data collection practices.

110. Along with specificity and volume, Facebook also obfuscates the type of information it collects. Facebook allows advertisers, like the Streaming Services, to manually upload customer lists to Facebook's ad system.[122] The customer lists must contain "'identifier[s]' (such as email, phone number, address),"[123] thereby allowing Facebook to link to "profiles so that [advertisers] can advertise to [their] customers on Facebook, Instagram and Audience Network."[124] That way, when advertisers create an ad campaign, Facebook can "match the offline data [they] upload to the event set so that [they] can see how much [their] ads resulted in offline activity."[125] Facebook recommends timestamping this event data "to the minute or second."

---

[120] *See* Figure 18.
[121] *Compare with* Figure 1.
[122] FACEBOOK, CREATE A CUSTOMER LIST CUSTOM AUDIENCE, https://www.facebook.com/business/help/170456843145568?id=2469097953376494
[123] *Id.*
[124] FACEBOOK, ABOUT CUSTOMER LIST CUSTOM AUDIENCES, https://www.facebook.com/business/help/341425252616329?id=2469097953376494
[125] FACEBOOK, UPLOAD OFFLINE EVENT DATA, https://www.facebook.com/business/help/155437961572700?id=565900110447546.

111. Customer lists help Facebook catch a user's off-site activity that an advertiser's Business Tools, like the Streaming Services' Business Tools, cannot collect.

112. Because the Off-Facebook Activity report is "a summary of activity that businesses and organisations share with us about your interactions with them," the data Facebook collects from customer lists should be included in that report. Likewise, when a user disables Facebook's ability to collect Off-Facebook Activity, that should also apply to off-site activity collected through customer lists. Both presumptions are incorrect.

113. Disabling off-Facebook activity has no impact on customer list data. In fact, to exercise any control over information from lists, users must navigate to an entirely different part of Facebook's website.

To turn off your future off-Facebook activity for all apps and websites:

1. Click in the top right of Facebook.
2. Select **Settings & Privacy**, then click **Settings**.
3. Click **Your Facebook Information** in the left column, then click **Off-Facebook Activity**.
4. Click **Manage Your Off-Facebook Activity**, then click **Manage Future Activity**.
5. Click **Manage Future Activity**.
6. Click next to **Future Off-Facebook Activity**, then click **Turn Off** to turn off your future off-Facebook activity.

114. Should a user somehow intuit this distinction and successfully navigate to Ad Preferences, Facebook still provides little reprieve. For customer lists, users can exercise control over an advertiser's event data, meaning "data that advertisers and other partners provide to us about your activity on their websites and apps, as well as some of your offline interactions, such as

purchases."[126] But Facebook still helps advertisers match identifiers contained in customer lists with users' Facebook profiles, even when those users have disabled personalized ads. For this feature, Facebook, unlike how it handles event data, offers users no control and lets advertisers use this information to build audiences.

115. These omissions and misrepresentations are contrary to Facebook's terms and representations. Facebook emphasizes to users that they can control and review the data Facebook collects. Facebook's Terms of Service informs users they "have controls over the types of ads and advertisers you see, and the types of information we use to determine which ads we show you."[127] Facebook's Cookies Policy states users can "use your ad preferences to learn why you're seeing a particular ad and control how we use information that we collect to show you ads."[128] If users wish to review the data Facebook collects, the Cookies Policy recommends "review[ing] your Off-Facebook activity, which is a summary of activity that businesses and organisations share with us about your interactions with them, such as visiting their apps or websites."[129] And Facebook's Data Policy tells users they can exercise "choices over the data we use to select ads and other sponsored content for you in the Facebook Settings and Instagram Settings."[130] But as set forth, Facebook's tools for controlling and reviewing its data collection practices are incomplete, inaccurate, and intentionally designed to deceive and confuse users.

116. Like any transaction, the terms between users and Facebook must be fairly disclosed, not misrepresented. Users exchange activity and permissions for access to Facebook's platform. By misrepresenting users' ability to review and control how their activity is collected, Facebook misrepresents terms that form the basis of the bargain, leaving users unable to properly assent or consent.

---

[126] FACEBOOK, HOW CAN I ADJUST HOW ADS ON FACEBOOK ARE SHOWN TO ME BASED ON DATA ABOUT MY ACTIVITY FROM PARTNERS?, https://www.facebook.com/help/568137493302217.
[127] FACEBOOK, TERMS OF SERVICE, https://www.facebook.com/terms.php.
[128] FACEBOOK, COOKIES & OTHER STORAGE TECHNOLOGIES, https://www.facebook.com/policies/cookies.
[129] *Id.*
[130] FACEBOOK, DATA POLICY, https://www.facebook.com/policy.php.

CLASS ACTION ALLEGATIONS

117. Plaintiffs bring this class action on behalf of all persons with Facebook accounts who subscribe to Paramount+, ESPN+, Hulu, and Starz (the "Class").

118. Plaintiff Starzinski also brings this suit on behalf of all persons with a Paramount+ subscription (the "Paramount Subclass").

119. Plaintiff Odumosu also brings this suit on behalf of all persons with an ESPN+ subscription (the "ESPN Subclass").

120. Plaintiffs Odumosu and Medina also bring this suit on behalf of all persons with a Hulu subscription (the "Hulu Subclass").

121. Plaintiff McCoy also brings this suit on behalf of all persons with a Starz subscription (the "Starz Subclass").

122. Excluded from the Classes are Defendant, the officers and directors of the Defendant at all relevant times, members of their immediate families and their legal representatives, heirs, successors or assigns and any entity in which either Defendant have or had a controlling interest.

123. Plaintiffs are members of the Class and Subclasses they seek to represent.

124. Members of the putative class and subclass are so numerous that their individual joinder herein is impracticable. On information and belief, members of the putative class and number in the millions. The precise number of putative class members and their identities are unknown to Plaintiffs at this time but may be determined through discovery. Putative class members may be notified of the pendency of this action by mail and/or publication through the distribution records of Defendant.

125. Common questions of law and fact exist as to all putative class and subclass members and predominate over questions affecting only individual class members. Common legal and factual questions include, but are not limited to:

a. Whether Facebook represented to Class and Subclass members that it would not collect sensitive, confidential, protected, or unlawfully disclosed information;

b. Whether Facebook represented to Class and Subclass members that they could control and review the activity Facebook collected and analyzed outside of the Facebook platform;

c. Whether Facebook gave the Class and Subclass a reasonable expectation of privacy that their communications of personally identifiable information, as defined by the VPPA, were not being intercepted, received, or collected by Facebook when they accessed and ordered video content through the Streaming Services;

d. Whether Facebook gave the Class and Subclass members a reasonable expectation of privacy that any communications with a video content provider with which they subscribed, like the Streaming Services, were not being intercepted, received, or collected by Facebook;

e. Whether Facebook in fact intercepted, received, or collected communications from Class and Subclass members when those members communicated generally with the Streaming Services or were transmitting personally identifiable information to the Streaming Services;

f. Whether Facebook in fact intercepted, received, or collected communications from Class and Subclass when Class and Subclass members communicated with websites that integrated Facebook's Business Tools;

g. Whether Facebook's practice of intercepting, receiving, or collecting communications of personally identifiable information or other communications between the Streaming Services and Class and Subclass members violated state and federal privacy laws;

h. Whether Facebook's practice of intercepting, receiving, or collecting electronic communications violated state and federal privacy laws;

i. Whether Facebook's practice of intercepting, receiving, or collecting communications of personally identifiable information or other communications

between the Streaming Services and Class and Subclass members violated state and federal anti-wiretapping laws;

j. Whether Facebook's practice of intercepting, receiving, or collecting electronic communications violated state and federal anti-wiretapping laws;

k. Whether Plaintiffs and Class members are entitled to declaratory and/or injunctive relief to enjoin the unlawful conduct alleged herein; and

l. Whether Plaintiffs and Class members have sustained damages as a result of Facebook's conduct and if so, what is the appropriate measure of damages or restitution.

126. Plaintiffs' claims are typical of the claims of the members of the Classes as all members of the Classes are similarly affected by Defendant's wrongful conduct. Plaintiffs have no interests antagonistic to the interests of the other members of the Classes. Plaintiffs and all members of the Classes have sustained economic injury arising out of Defendant's violations of common and statutory law as alleged herein.

127. Plaintiffs are adequate representatives of the Classes because their interests do not conflict with the interests of the putative class members they seek to represent, they have retained counsel competent and experienced in prosecuting class actions, and they intend to prosecute this action vigorously. The interests of the Classes will be fairly and adequately protected by Plaintiffs and their counsel.

128. The class mechanism is superior to other available means for the fair and efficient adjudication of the claims of Plaintiffs and the putative members of the Classes. Each individual Class member may lack the resources to undergo the burden and expense of individual prosecution of the complex and extensive litigation necessary to establish Defendant's liability. Individualized litigation increases the delay and expense to all parties and multiplies the burden on the judicial system presented by the complex legal and factual issues of this case. Individualized litigation also presents a potential for inconsistent or contradictory judgments. In contrast, the class action device presents far fewer management difficulties and provides the benefits of single adjudication, economy of scale, and comprehensive supervision by a single court on the issue of Defendant's

liability. Class treatment of the liability issues will ensure that all claims are consistently adjudicated.

129. California law applies to the entirety of the Classes. California's substantive laws apply to every member of the Classes, regardless of where in the United States the Class member resides. Defendant's own Terms of Service explicitly state that "the laws of the State of California will govern these Terms and any claim, without regard to conflict of law provisions." By choosing California law for the resolution of disputes covered by its Terms of Service, Facebook concedes that it is appropriate for this Court to apply California law to the instant dispute to all Class members. Further, California's substantive laws may be constitutionally applied to the claims of Plaintiffs and the Class members under the Due Process Clause, *see* U.S. Const. amend. XIV, § 1, and the Full Faith and Credit Clause, *see* U.S. Const. art. IV, § 1, of the U.S. Constitution. California has significant contact, or significant aggregation of contacts, the claims asserted by the Plaintiffs and all Class members, thereby creating state interests that ensure that the choice of California state law is not arbitrary or unfair. Defendant's decision to reside in California and avail itself of California's laws, and to engage in the challenged conduct from and emanating out of California, renders the application of California law to the claims herein constitutionally permissible. The application of California laws to the Classes is also appropriate under California's choice of law rules because California has significant contacts to the claims of Plaintiffs and the proposed Classes and California has the greatest interest in applying its laws here.

130. Plaintiffs reserve the right to revise the foregoing class allegations and definitions based on facts learned and legal developments following additional investigation, discovery, or otherwise.

COUNT I
Violation Of The Federal Wiretap Act, 18 U.S.C. § 2510, *et seq.*
(The Class and Subclasses)

131. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

132. The Federal Wiretap Act, as amended by the Electronic Communications Privacy Act of 1986, prohibits the intentional interception of the contents of any wire, oral, or electronic communications through the use of a device. 18 U.S.C. § 2511.

133. The Wiretap Act protects both the sending and receiving of communications.

134. 18 U.S.C. § 2520(a) provides a private right of action to any person whose wire, oral or electronic communication is intercepted.

135. Facebook's actions in intercepting and tracking communications between the Streaming Services and subscribers containing subscribers' personally identifiable information, as defined by the VPPA, was intentional. On information and belief, Facebook is aware that it is intercepting communications in these circumstances and has taken no remedial action.

136. Facebook's actions in intercepting and tracking electronic communications were intentional. On information and belief, Facebook is aware that it is intercepting communications in these circumstances and has taken no remedial action.

137. Facebook's intentional interception of internet communications that Plaintiffs and Class members were sending and receiving while navigating websites that integrated Facebook's Business Tools was done contemporaneously with the Plaintiffs' and Class and Subclass members' sending and receipt of those communications.

138. Facebook's interception of internet communications that Class and Subclass members and Plaintiffs were sending and receiving while on the Streaming Services was done contemporaneously with Plaintiffs' and Class members' sending and receipt of those communications.

139. The communications intercepted by Facebook included "contents" of electronic communications made from Plaintiffs and Class and Subclass members. These communications include those sent and received by Plaintiffs and Class and Subclass members containing detailed URL requests.

140. The communications intercepted by Facebook included "contents" of electronic communications made from Plaintiffs and Class and Subclass members to the Streaming Services. These communications include those sent and received by Plaintiffs and Class and Subclass

members containing detailed URL requests, form field entries like email address and name, button clicks and associated text, and a complete transcription of the subscriber's communicated request, down to the videos that the subscribers asked the Streaming Services to deliver.

141. The transmission of data between Plaintiffs and Class members were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photo optical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

142. The following constitute "devices" within the meaning of 18 U.S.C. 2510(5):

a. The computer codes and programs Facebook used to track Plaintiffs' and the Class members' communications while they were navigating websites that integrated Facebook's Business Tools;

b. Plaintiffs' and Class member's browsers, mobile applications, and television applications;

c. Plaintiffs' and Class and Subclass members' computing, streaming, and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to navigate platforms that integrated Facebook's Business Tools;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were navigating platforms that integrated Facebook's Business Tools; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' electronic communications.

143. The transmission of data between Plaintiffs and Class and Subclass members and the Streaming Services while subscribing, logging in, selecting videos and watching videos were "transfer[s] of signs, signals, writing, … data, [and] intelligence of [some] nature transmitted in whole or in part by a wire, radio, electromagnetics, photoelectronic, or photooptical system that affects interstate commerce[,]" and were therefore "electronic communications" within the meaning of 18 U.S.C. § 2510(12).

144. The following constitute "devices" within the meaning of 18 U.S.C. 2510(5):

a. The computer codes and programs Facebook used to track Plaintiffs' and Class and Subclass members' communications while they were subscribing to the Streaming Services, logging into the Streaming Services, and selecting and watching videos on the Streaming Services;

b. Plaintiffs' and Class and Subclass members' browsers, mobile applications, and television applications;

c. Plaintiffs' and Class and Subclass members' computing, streaming, and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were

using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services.

145. Facebook, in its conduct alleged here, was not providing an "electronic communication service," as that term is defined in 18 U.S.C. § 2510(12) and is used elsewhere in the Wiretap Act. Facebook was not acting as an Internet Service Provider ("ISP"). The conduct alleged here does not arise from Facebook's separate instant messenger business.

146. Facebook also was not an authorized party to the communications because Plaintiffs and Class and Subclass members were unaware of Facebook's redirecting of the referrer URL, form field entries, or communication transcriptions to Facebook itself, did not knowingly send any communication to Facebook, were accessing content on the internet, when Facebook intercepted the communications from Plaintiffs. Facebook could not manufacture its own status as a party to Plaintiffs' and Class and Subclass members' communications with others by surreptitiously redirecting or intercepting those communications.

147. Facebook was not an authorized party to the communications because Plaintiffs and Class and Subclass members were unaware of Facebook's redirecting of the referrer URL, form field entries, or communication transcriptions to Facebook itself, did not knowingly send any communication to Facebook, were accessing and ordering video content while logged into their Streaming Services subscriptions, when Facebook intercepted the communications between Plaintiffs and the Streaming Services. Facebook could not manufacture its own status as a party to Plaintiffs' and Class and Subclass members' communications with others by surreptitiously redirecting or intercepting those communications.

148. As illustrated herein, the communications between Plaintiffs and Class members on the one hand, and websites on the other, were simultaneous to, but *separate from*, the channel through which Facebook acquired the contents of those communications.

149. Plaintiffs and Class and Subclass members did not consent to Facebook's interception or continued gathering of the user's communications after accessing a platform that integrated Facebook's Business Tools because Facebook obfuscated the data it collected and users had no ability to check Facebook's claims.

150. Plaintiffs and Class and Subclass members did not consent to Facebook's interception or continued gathering of the user's communications after accessing a video tape service provider's platform, where Plaintiffs and Class and Subclass members then logged into their Streaming Services subscription and ordered and watched videos. Indeed, Facebook represented to Plaintiffs and Class and Subclass members, and the public at large, that it would not collect sensitive or protected information unless authorized by the user. Moreover, the communications intercepted by Facebook were plainly confidential, which is evidenced by the numerous state and federal statutes that protect a subscriber's video-viewing history from being disclosed.

151. The interception by Facebook in the aforementioned circumstances were unlawful and tortious.

152. After intercepting the communications, Facebook then used the contents of the communications knowing or having reason to know that such information was obtained through the interception of electronic communications in violation of 18 U.S.C. § 2511(a).

153. As the result of the above actions and pursuant to 18 U.S.C. § 2520, the Court may assess statutory damages to Plaintiffs and Class and Subclass members; injunctive and declaratory relief; punitive damages in an amount to be determined by a jury, but sufficient to prevent the same or similar conduct by Facebook in the future, and a reasonable attorney's fee and other litigation costs reasonably incurred.

COUNT II
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 631
(The Class and Subclasses)

154. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

155. Plaintiffs bring this Count individually and on behalf of the members of the Class and Subclasses.

156. The California Invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose.

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> Cal. Penal Code § 630.

157. California Penal Code § 631(a) provides, in pertinent part:

> Any person who, by means of any machine, instrument, or contrivance, or in any other manner … willfully and without the consent of all parties to the communication, or in any unauthorized manner, reads, or attempts to read, or to learn the contents or meaning of any message, report, or communication while the same is in transit or passing over any wire, line, or cable, or is being sent from, or received at any place within this state; or who uses, or attempts to use, in any manner, or for any purpose, or to communicate in any way, any information so obtained, or who aids, agrees with, employs, or conspires with any person or persons to unlawfully do, or permit, or cause to be done any of the acts or things mentioned above in this section, is punishable by a fine not exceeding two thousand five hundred dollars ($2,500).

158. A defendant must show it had the consent of <u>all</u> parties to a communication.

159. Facebook has its principal place of business in California; designed, contrived and effectuated its scheme to track its users generally and track users who logged into a subscription-based platform for a video service provider and accessed and watched videos; and has adopted California substantive law to govern its relationship with its users.

160. At all relevant times, Facebook's tracking and interceptions of Plaintiffs' and Class and Subclass members' internet communications while accessing platforms that integrated Facebook's Business Tools was without authorization and consent from Plaintiffs and Class and Subclass members. The interceptions by Facebook in the aforementioned circumstances were unlawful and tortious.

161. At all relevant times, Facebook's tracking and interceptions of Plaintiffs' and Class and Subclass members' internet communications while accessing and watching videos on the Streaming Services was without authorization and consent from Plaintiffs and Class and Subclass members. The interceptions by Facebook in the aforementioned circumstances were unlawful and tortious.

162. Facebook's non-consensual tracking of Plaintiffs' and Class and Subclass members' internet communications who were accessing a platform that integrated Facebook's Business Tools was designed to attempt to learn at least some meaning of the content in the URLs and the content of the materials requested.

163. Facebook's non-consensual tracking of Plaintiffs' and Class and Subclass members' internet communications who were accessing and watching videos on the Streaming Services was designed to attempt to learn at least some meaning of the content in the URLs and the content of the videos requested.

164. The following items also constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Facebook's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Facebook used to track Plaintiffs' and Class members' communications while they were navigating websites that integrated Facebook's Business Tools;

b. Plaintiffs' and Class and Subclass members' browsers, mobile applications, and television applications;

c. Plaintiffs' and Class and Subclass members' computing, streaming, and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to navigate platforms that integrated Facebook's Business Tools;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were navigating platforms that integrated Facebook's Business Tools; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' electronic communications.

165. The following items constitute "machine[s], instrument[s], or contrivance[s]" under the CIPA, and even if they do not, Facebook's deliberate and admittedly purposeful scheme that facilitated its interceptions falls under the broad catch-all category of "any other manner":

a. The computer codes and programs Facebook used to track Plaintiffs' and Class and Subclass members' communications while they were subscribing to the Streaming Services, logging into the Streaming Services, and selecting and watching videos on the Streaming Services;

b. Plaintiffs' and Class and Subclass members' browsers, mobile applications, and television applications;

c. Plaintiffs' and Class and Subclass members' computing, streaming, and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services.

166. Plaintiffs and Class and Subclass members have suffered loss by reason of these violations, including, but not limited to, violations of their rights of privacy, loss of value in their electronic communications, and loss of value in their personally-identifiable information.

167. Pursuant to California Penal Code § 637.2, Plaintiffs and Class and Subclass members have been injured by the violation of California Penal Code § 631 and each seek damages for the greater of $5,000 or three times the actual amount of damages, as well as injunctive relief.

COUNT III
Violation Of The California Invasion Of Privacy Act,
Cal. Penal Code § 632
(The Class and Subclasses)

168. Plaintiffs repeat the allegations contained in the paragraphs above as if fully set forth herein.

169. Plaintiffs bring this Count individually and on behalf of the members of the Class and Subclasses.

170. The California invasion of Privacy Act ("CIPA") is codified at Cal. Penal Code §§ 630 to 638. The Act begins with its statement of purpose

> The Legislature hereby declares that advances in science and technology have led to the development of new devices and techniques for the purpose of eavesdropping upon private communications and that the invasion of privacy resulting from the continual and increasing use of such devices and techniques has created a serious threat to the free exercise of personal liberties and cannot be tolerated in a free and civilized society.
>
> Cal. Penal Code § 630.

171. California Penal code § 632(a) provides, in pertinent part:

> A person who, intentionally and without the consent of all parties to a confidential communication, uses an electronic amplifying or recording device to eavesdrop upon or record the confidential communication, whether the communication is carried on among the parties in the presence of one another or by means of a telegraph, telephone, or other device, except a radio, shall be punished by a fine not exceeding two thousand five hundred dollars ($2,500) per violation.

172. A defendant must show it had the consent of <u>all</u> parties to a communication.

173. The following items constitute "an electronic amplifying or recording device" under the CIPA:

a. The computer codes and programs Facebook used to track Plaintiffs' and Class and Subclass members' communications while they were subscribing to the Streaming Services, logging into the Streaming Services, and selecting and watching videos on the Streaming Services;

b. Plaintiffs' and Class and Subclass members' browsers, mobile applications, and television applications;

c. Plaintiffs' and Class and Subclass members' computing, streaming, and mobile devices;

d. Facebook's web and ad servers;

e. The web and ad-servers from which Facebook tracked and intercepted Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services;

f. The computer codes and programs used by Facebook to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services; and

g. The plan Facebook carried out to effectuate its tracking and interception of Plaintiffs' and Class and Subclass members' communications while they were using a web browser, mobile application, or television application to subscribe to, access, or watch videos on the Streaming Services.

174. The data collected by Facebook constitutes "confidential communications," as that term is used in Section 632, because Plaintiffs and Class and Subclass members had objectively reasonable expectations of privacy while ordering and accessing videos on the Streaming Services.

175. Pursuant to Cal. Penal Code § 637.2, Plaintiffs and Class and Subclass members have been injured by the violations of Cal. Penal Code § 635, and each seek damages for the greater of $5,000 or three times the amount of actual damages, as well as injunctive relief.

PRAYER FOR RELIEF

WHEREFORE, Plaintiffs prays for relief and judgment, as follows:

a. Determining that this action is a proper class action;

b. For an order certifying the Classes, naming Plaintiffs as representatives of the Class and Subclasses, and naming Plaintiffs' attorneys as Class Counsel to represent the Class and Subclasses;

c. For an order declaring that Defendant's conduct violates the statutes referenced herein;

d. For an order finding in favor of Plaintiffs and the Class and Subclasses on all counts asserted herein;

e. Award compensatory damages, including statutory damages where available, to Plaintiffs and the Class and Subclass members against Defendant for all damages sustained as a result of Defendant's wrongdoing, in an amount to be proven at trial;

f. For punitive damages, as warranted, in an amount to be determined at trial;

g. Ordering Defendant to disgorge revenues and profits wrongfully obtained;

h. For prejudgment interest on all amounts awarded;

i. For injunctive relief as pleaded or as the Court may deem proper;

j. For an order awarding Plaintiffs and the Class their reasonable attorneys' fees and expenses and costs of suit; and

k. Grant Plaintiffs and the Class and Subclass members such further relief as the Court deems appropriate.

DEMAND FOR TRIAL BY JURY

Plaintiffs hereby demand a trial by jury of all issues so triable.

Dated: June 27, 2024

Respectfully submitted,

BURSOR & FISHER, P.A.

By: _____

Philip L. Fraietta (State Bar No. 354768)
1330 Avenue of the Americas
New York, NY 10019
Telephone: (646) 837-7150
Facsimile: (212) 989-9163
E-mail: pfraietta@bursor.com

BURSOR & FISHER, P.A.
L. Timothy Fisher (State Bar No. 191626)
1990 North California Blvd., Suite 940
Walnut Creek, CA 94596
Telephone: (925) 300-4455
Facsimile: (925) 407-2700
Email: ltfisher@bursor.com

Attorneys for Plaintiffs